

UNITED STATES DISTRICT COURT

for the  
Southern District of Ohio

FILED  
RICHARD W. NAGEL  
CLERK OF COURT

2018 DEC 13 PM 4:04

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)

SIX (6) SD CARDS (SUBJECT DEVICES C), STORED  
AT HSI, 9875 REDHILL DRIVE, BLUE ASH, OHIO  
45242

Case No.

3:18-mj-00808  
MICHAEL J. NEWMAN

APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

SEE ATTACHMENT C

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me and signed in my presence.

Date: 12/13/18

City and state: DAYTON, OHIO

Applicant's signature  
SA CHRISTOPHER WALLACE, HSI  
Printed name and title

Judge's signature  
MICHEL J. NEWMAN, U.S. MAGISTRATE JUDGE  
Printed name and title

**ATTACHMENT A**

The property to be searched is:

1. REPUBLIC OF GAMING COMPUTER TOWER, SERIAL NUMBER F9PDCG000HK0 (SUBJECT DEVICE A);
2. CUSTOM BUILT COMPUTER TOWER (SUBJECT DEVICE B);
3. 6 SD CARDS (SUBJECT DEVICES C);
4. 2 FLASH MEMORY STORAGE DRIVES (SUBJECT DEVICES D);
5. 2 EXTERNAL HARD DRIVES HA0N33TE (SUBJECT DEVICES E);
6. OLYMPUS DIGITAL CAMERA, MODEL NUMBER FE-115 (SUBJECT DEVICE F);
7. 11 INTERNAL HARD DRIVES (SUBJECT DEVICES G);
8. HP LAPTOP, SERIAL NUMBER 5CB0500WGJ (SUBJECT DEVICE H);

The SUBJECT DEVICES are currently stored in a secure locker in the HOMELAND SECURITY INVESTIGATIONS OFFICE LOCATED AT 9875 REDHILL DRIVE, BLUE ASH, OHIO 45242

This warrant authorizes the forensic examination of SUBJECT DEVICES for the purpose of identifying the electronically stored information described in Attachment B.

## **ATTACHMENT B**

All records on the SUBJECT DEVICES described in Attachment A that relate to violations of 18 U.S.C. §§ 2252(a)(4)(B), 2252A(a)(5)(B), 2252(a)(2), and 2252A(a)(2) (possession, receipt, and distribution of child pornography), including but not limited to the following:

- a. Any visual depictions and records related to the possession, receipt, and distribution of child pornography;
- b. Any visual depictions of minors;
- c. Any Internet history indicative of searching for child pornography;
- d. Any Internet communications (including email, social media, and online chat programs) with others in which child exploitation materials and offenses are discussed and/or traded, and any contact / identifying information for these individuals;
- e. Any Internet communications (including email, social media, and online chat programs) with minors, and any contact / identifying information for these minors;
- f. Evidence of utilization of email accounts, social media accounts, online chat programs, and Peer-to-Peer file sharing programs, including any account / user names;
- g. Evidence of utilization of the name "PyroBane" and any aliases or fictitious names;
- h. Any information related to Internet Protocol (IP) addresses and Wi-Fi accounts accessed by the SUBJECT DEVICES;
- i. Evidence of user attribution showing who used or owned the SUBJECT DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage and any photographic form.

The authorization includes the seizure and search of electronic data to include deleted data, remnant data and slack space.

**ATTACHMENT C**

<u>Code Section</u>	<u>Offense Description</u>
18 U.S.C. § 2252(a)(4)(B)	Possession of Child Pornography
18 U.S.C. § 2252A(a)(5)(B)	Possession of Child Pornography
18 U.S.C. § 2252(a)(2)(B)	Receipt and Distribution of Child Pornography
18 U.S.C. § 2252A(a)(2)	Receipt and Distribution of Child Pornography



**AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS**

1. I, Special Agent (SA) Christopher Wallace, being duly sworn under oath, do hereby depose and state:

2. I am a Special Agent with Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), and I have been so employed since May of 2005. As part of my daily duties as an HSI agent, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the distribution, receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252(a) and 2252A. I have received training in the area of child pornography and child exploitation. I have additionally had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have also participated in the execution of numerous search warrants, a number of which involved child exploitation and/or child pornography offenses.

3. This affidavit is being made in support of an application for a search warrant for the following electronic devices which were seized on December 6, 2018 from a residence located at 1046 1/2 Caldwell Street, Piqua, Ohio by law enforcement authorities:

- a. Republic of Gaming computer tower, serial number F9PDCG000HK0 (SUBJECT DEVICE A);
- b. Custom built computer tower (SUBJECT DEVICE B);
- c. 6 SD cards (SUBJECT DEVICES C);
- d. 2 Flash memory storage drives (SUBJECT DEVICES D);
- e. 2 External hard drives HA0N33TE (SUBJECT DEVICES E);
- f. Olympus Digital Camera, model number FE-115 (SUBJECT DEVICE F);
- g. 11 Internal hard drives (SUBJECT DEVICES G);

h. HP laptop, serial number 5CB0500WGJ (SUBJECT DEVICE H);  
currently located at the Department of Homeland Security, 9875 Redhill Drive, Blue Ash, Ohio, 45242, and as more fully described in Attachment A.

4. The purpose of this search warrant request is to search and seize evidence stored on electronic media, more particularly described in Attachment B, which is considered to be violations of 18 U.S.C. §§ 2252(a)(4)(B) and 2252A(a)(5)(B), which make it a crime to possess child pornography and access child pornography with intent to view it, and violations of 18 U.S.C. §§ 2252(a)(2)(B) and 2252A(a)(2), which make it a crime to receive and distribute child pornography. The items to be searched for and seized are described more particularly in Attachment B hereto.

5. The statements contained in this Affidavit are based in part on my personal investigation of this matter and on information provided to me by other law enforcement agents. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have elected to set forth only those facts that I believe are necessary to establish probable cause to search for evidence of violations of 18 U.S.C. §§ 2252 and 2252A which is believed to be present within stored data located on the SUBJECT DEVICES.

6. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of federal law, including 18 U.S.C. §§ 2252 and 2252A, are present within the stored data located on the SUBJECT DEVICES.

**RELEVANT STATUTES**

7. 18 U.S.C. § 2252(a)(2)(B) states that it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mail if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

8. 18 U.S.C. § 2252A(a)(2) states that it is a violation for any person to receive or distribute – (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce, shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce, shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

9. 18 U.S.C. § 2252(a)(4)(B) states that it is a violation for any person to knowingly possess, or knowingly access with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

10. 18 U.S.C. § 2252A(a)(5)(B) states that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

11. For purposes of these statutes, the term “sexually explicit conduct” is defined in 18 U.S.C. § 2256(2) as:

- a. “Actual or simulated –
  - i. Sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;
  - ii. Bestiality;
  - iii. Masturbation;
  - iv. Sadistic or masochistic abuse; or
  - v. Lascivious exhibition of genitals or pubic area of any person.”

### **BACKGROUND INFORMATION**

#### **Definitions**

12. “**Child Pornography**” includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).



13. “**Visual depictions**” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

14. “**Child Erotica**” means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

15. “**Minor**” means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

16. “**Sexually explicit conduct**” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

17. “**Internet Service Providers**” or “**ISPs**” are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

18. An “**Internet Protocol address**”, also referred to as an “**IP address**”, is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as “octets,” ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).

19. A network “**server**,” also referred to as a “**host**,” is a computer system that has been designated to run a specific server application or applications and provide requested services to a “client” computer. A server can be configured to provide a wide variety of services over a network, including functioning as a web server, mail server, database server, backup server, print server, FTP (File Transfer Protocol) server, DNS (Domain Name System) server, to name just a few.

20. A “**client**” is the counterpart of a server or host. A client is a computer system that accesses a remote service on another computer by some kind of network. Web browsers (like Internet Explorer or Safari) are clients that connect to web servers and retrieve web pages for display. E-mail clients (like Microsoft Outlook or Eudora) retrieve their e-mail from their Internet service provider's mail storage servers.

21. “**Domain Name**” refers to the common, easy to remember names associated with an Internet Protocol address. For example, a domain name of “www.usdoj.gov” refers to the

Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first level or top-level domains are typically “.com” for commercial organizations, “.gov” for the governmental organizations, “.org” for organizations, and, “.edu” for educational organizations. Second level names will further identify the organization, for example “usdoj.gov” further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, “www.usdoj.gov” identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government. The Domain Name System, also referred to DNS, is a system of servers connected to each other using a common system of databases that resolve a particular domain name, such as “www.usdoj.gov,” to its currently assigned IP address (*i.e.*, 149.101.1.32), to enable the follow of traffic across the Internet.

22. **“Log Files”** are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

23. **“Hyperlink”** (often referred to simply as a “link”) refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. “resource”) to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.



24. “**Website**” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

25. “**Uniform Resource Locator**” or “**Universal Resource Locator**” or “**URL**” is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website’s home page file in the Web browser’s address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

26. “**Peer-to-Peer**” (P2P) file sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up file(s) on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user’s computer and conducting a search for files being shared on the network.

27. The terms “**records**”, “**documents**”, and “**materials**”, as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing,



typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

Characteristics of Collectors of Child Pornography

28. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereafter “collectors”):

a. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.

b. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature and sexual aids.

c. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.

d. Collectors almost always possess and maintain their “hard copies” of child pornographic images and reference materials (*e.g.*, mailing and address lists) in a private and secure location. With the growth of the Internet and computers, a large percentage of most collections today are in digital format. Typically these materials are kept at the collector’s residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods of time, even for years. Collectors often discard child pornography images only while “culling” their collections to improve their overall quality.

e. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.

f. Collectors prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

g. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation

between subscription and collection behavior has been repeatedly confirmed during several recent nationwide law enforcement initiatives.

Use of Computers and the Internet with Child Pornography

29. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other, as well the methods that individuals will use to interact with and sexually exploit children. Computers serve four functions in connection with child pornography: production; communication; distribution and storage.

a. **Production:** Pornographers can now produce both still and moving images directly from a common video camera. The camera is attached, using a cable, directly to the computer using a device called a video capture board. This device turns the video output into a form that is usable by computer programs. The output of the video camera can be stored, manipulated, transferred or printed directly from the computer. The captured image can be edited (*i.e.*, lightened, darkened, cropped, digitally enhanced, *etc.*) with a variety of commonly available graphics programs. The producers of child pornography can also use scanners to convert hard-copy photographs into digital images.

b. **Communication.** Previously, child pornography collectors had to rely on personal contact, U.S. mail, and telephonic communications in order to sell, trade, or market pornography. Today most communications associated with the trafficking of child pornography occur via the obscurity and relative anonymity of the Internet. A device known as a modem allows any computer to connect to the Internet via telephone lines or broadband Internet connections. Once connected to the Internet, individuals search for and/or offer to distribute child pornography in a wide variety of ways. Many individuals congregate in topic-based Internet chat rooms implicitly



or explicitly dedicated to child pornography. Online discussions in these chat rooms are usually done via instant message (or “IM”), and individuals may then establish one-on-one chat sessions involving private messages (or “PMs”), visible only to the two parties, to trade child pornography. These child pornography images may be attachments to the PMs, or they may be sent separately via electronic mail between the two parties. Pedophile websites communicate advertisements for the sale of child pornography, and individuals may order child pornography from these websites using email or send order information from their web browser (using HTTP computer language). Some individuals communicate via Internet Relay Chat (IRC) to discuss and trade child pornography images. It is not uncommon for child pornography collectors to engage in mutual validation of their interest in such material through Internet-based communications.

c. **Distribution.** Computers and the Internet are the preferred method to distribute child pornography. As discussed above, such images may be distributed via electronic mail (either as an attachment or embedded image), or through instant messages as attachments. Child pornography is regularly downloaded from servers or Usenet newsgroups via a method known as FTP (file transfer protocol). Child pornography images are also distributed from websites via client computers web browsers downloading such images via HTTP (Hyper Text Transfer Protocol). Peer-to-peer networks such as LimeWire and Gnutella are an increasingly popular method by which child pornography images are distributed over the Internet.

d. **Storage.** The computer's capability to store images in digital form makes it an ideal repository for pornography. A single floppy disk can store dozens of images and hundreds of pages of text. The size of computer hard drives used in home computers has grown tremendously within the last several years. Hard drives with the capacity of two hundred (200) gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Remote storage



of these images on servers physically removed from a collector's home computer adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

### **BACKGROUND OF INVESTIGATION**

30. The HSI Cyber Crimes Center, Child Exploitation Investigations Unit (C3 CEIU) received a referral from Russian law enforcement authorities via Interpol. The Cybercrime Department of the Russian Ministry of the Interior has been targeting users who share child pornography on Peer 2 Peer (P2P) networks. An individual with the username, "PyroBane" was identified by the Russian Cybercrime Department to have downloaded one child pornography video on May 29, 2018 from the IP address 24.165.117.88 (henceforth referred to as the TARGET IP ADDRESS). Open source researched conducted by C3 CEIU determined that the TARGET IP ADDRESS is operated by Charter Spectrum Communications.

31. On June 26, 2018, the C3 CEIU sent an administrative subpoena to Charter Spectrum Communications seeking subscriber information for the TARGET IP ADDRESS. Charter Spectrum Communications thereafter provided a response stating that the subject subscriber account was assigned to a Nathaniel Jones at 1046 1/2 Caldwell Street in Piqua, Ohio.

32. On December 6, 2018, SA Wallace and Piqua Police Department investigator Phillip Crusey traveled to 1046 1/2 Caldwell Street in Piqua, Ohio. SA Wallace and Investigator Crusey knocked at the door of 1046 1/2 Caldwell Street. No one answered the door. 1046 1/2 Caldwell Street is the 2<sup>nd</sup> floor unit of a duplex. SA Wallace and Investigator Crusey then encountered the first floor neighbors of Nathaniel Jones at 1046 Caldwell Street. The neighbors

stated that Nathaniel Jones was currently at the residence and agreed to call Jones and inform Jones that law enforcement officers were knocking at the door. After approximately 5 minutes, Jones eventually opened the front door of 1046 1/2 Caldwell and walked out onto the porch and closed the door behind him (Nathaniel Jones). SA Wallace identified himself as a Special Agent with HSI and asked Jones if he (Nathaniel Jones) was willing to answer questions inside Jones' residence. Jones asked SA Wallace what the questions would concern, and SA Wallace responded the questions would be about Jones' internet usage. Jones replied "OK," and led SA Wallace and Investigator Crusey into his residence.

33. During the interview, Jones admitted to using a file transfer website named "Wireshare" to download child pornography videos. Jones admitted to downloading 50 – 75 child pornography videos in the last four (4) to six (6) months and storing the child pornography videos on the Republic of Gaming computer tower, Serial Number F9PDCG000HK0 (SUBJECT DEVICE A). Jones stated that he (Nathaniel Jones) preferred videos of male children under the age of 13 engaging in sexual activity with other children. During the interview Jones was asked how many computers and electronic storage devices were used in the home and belonged to Jones. Jones listed the SUBJECT DEVICES A-H. Jones consented to having SUBJECT DEVICES A-H searched by HSI Special Agents and proceeded to sign a HSI consent to search form. Jones then escorted SA Wallace and Investigator Crusey through the residence and pointed out SUBJECT DEVICES A, B, C, D, E, F, G and H.

#### **ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

34. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the

Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

35. Nature of examination: Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the **SUBJECT DEVICES** consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the **SUBJECT DEVICES** to human inspection in order to determine whether it is evidence described by the warrant.

36. Manner of execution: Because the warrant seeks only permission to examine a device already in law enforcement's possession, the execution of the warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

//

//

//

//

//

//

//

//

//

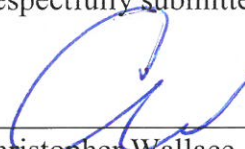
//

//

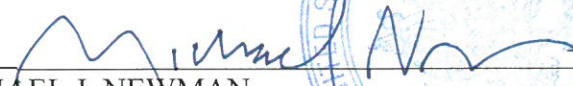
**CONCLUSION**

37. Based on the foregoing, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252(a)(2)(B) and 2252A(a)(2) (distribution and receipt of child pornography), and Title 18, United States Code, Sections 2252(a)(4)(B) and 2252A(a)(5)(B) (possession of child pornography) may be located on the **SUBJECT DEVICES**, as further described in Attachment A. I therefore respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

Respectfully submitted,

  
\_\_\_\_\_  
Christopher Wallace  
Special Agent  
Homeland Security Investigations

Sworn and subscribed before me this 13<sup>th</sup> day of  
December 2018, at Dayton, Ohio.

  
\_\_\_\_\_  
MICHAEL J. NEWMAN  
UNITED STATES MAGISTRATE JUDGE

